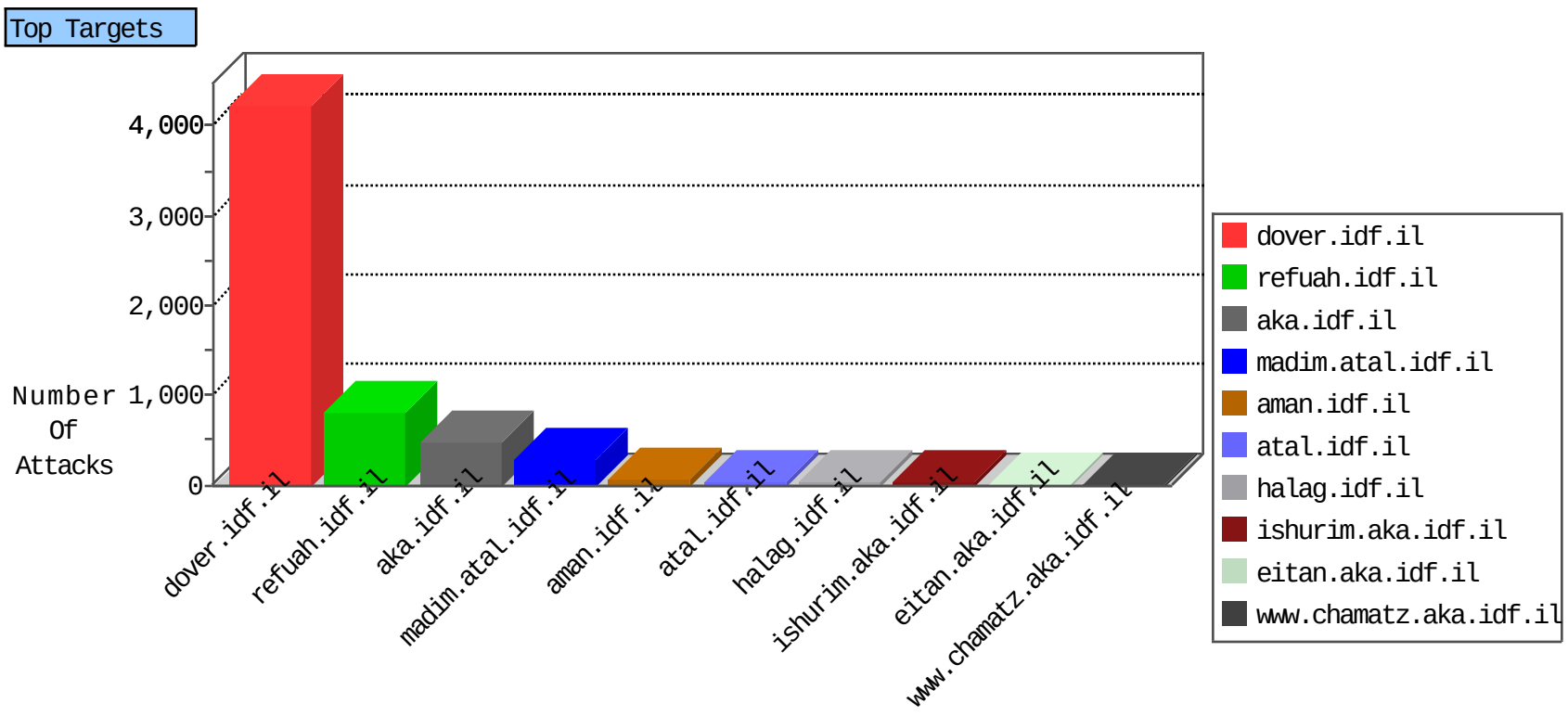
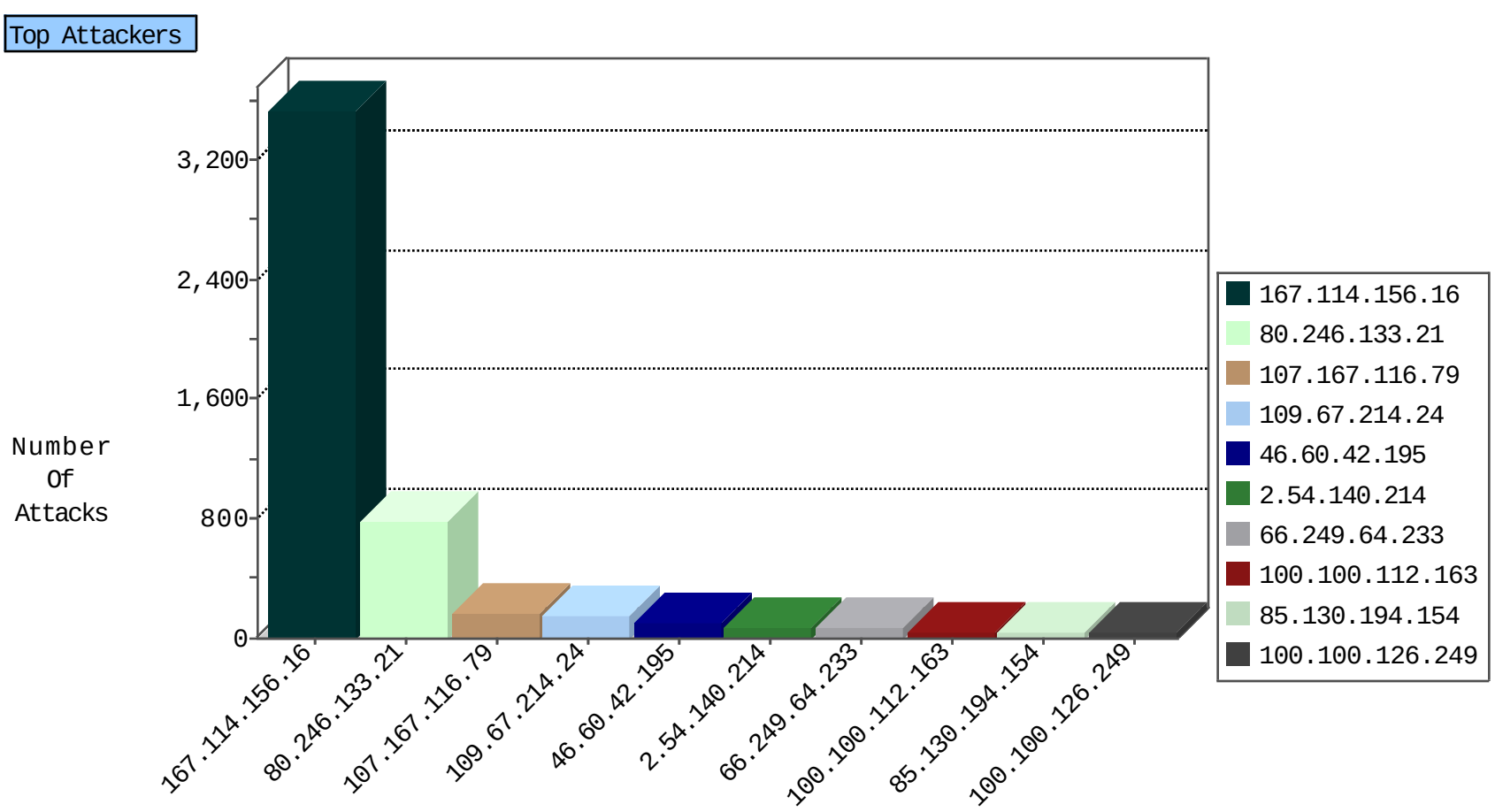
11-24-2015-22:04:05 to 11-24-2015-23:04:05

# IDF Under Attack Daily Report




Top Target




Top Attackers

11-24-2015-22:04:05 to 11-24-2015-23:04:05

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | DOS-Tool-SwitchbladG | dest-reset | 2717 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.il | HTTP Page Flood Attack | drop | 2 |
| 93.174.93.151 | Netherlands | 147.237.76.200 | eitan.aka.idf.il | Block_Udp_All_Nets | drop | 1 |

11-24-2015-22:04:05 to 11-24-2015-23:04:05

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|

11-24-2015-22:04:05 to 11-24-2015-23:04:05

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 10 |
| 195.34.150.18 | 147.237.77.216 | Austria | dover.idf.il | Tehila - Perl LWP with fake user agent | 3 |
| 169.54.233.119 | 147.237.8.24 | Netherlands | e.lifestyle.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.0.35 | Netherlands | akaws.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.0.15 | Netherlands | kosher-kravi.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 96.57.161.90 | 147.237.8.50 | United States | e.tikshuv.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 169.54.233.119 | 147.237.77.74 | Netherlands | law.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.244.49.137 | 147.237.76.197 | Hong Kong | e.himush.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 169.54.233.119 | 147.237.76.196 | Netherlands | e.sviva.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.76.44 | Netherlands | e.refuah.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.8.50 | Netherlands | e.tikshuv.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.8.27 | Netherlands | e.madim.atal.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.0.200 | Netherlands | m4u.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.0.19 | Netherlands | madim.atal.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 153.99.207.124 | 147.237.0.19 | China | madim.atal.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 169.54.233.119 | 147.237.77.212 | Netherlands | e.dover.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 66.131.229.16 | 147.237.77.216 | Canada | dover.idf.il | portscan: TCP Distributed Portscan | 1 |
| 169.54.233.119 | 147.237.77.19 | Netherlands | law-forum.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 61.130.145.216 | 147.237.77.216 | China | dover.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 169.54.233.119 | 147.237.76.177 | Netherlands | ncore.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 31.6.71.154 | 147.237.0.19 | Poland | madim.atal.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 169.54.233.119 | 147.237.76.39 | Netherlands | mobile.meitav.idf.i | ET SCAN Potential VNC Scan 5800-5820 | 1 |
| 169.54.233.119 | 147.237.8.46 | Netherlands | e.chinuch.idf.il | ET SCAN Potential VNC Scan 5800-5820 | 1 |

11-24-2015-22:04:05 to 11-24-2015-23:04:05

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 167.114.156.16 | Canada | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 1679 |
| 80.246.133.21 | Israel | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 782 |
| 107.167.116.79 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 131 |
| 66.249.64.233 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 66 |
| 107.167.116.79 | United States | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 39 |
| 85.130.194.154 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 100.100.126.249 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 34 |
| 100.100.112.163 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 27 |
| 66.249.81.218 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 37.142.181.229 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 24 |
| 46.19.85.14 | Israel | 147.237.72.167 | ishurim.aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 20 |
| 2.54.21.111 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 20 |
| 66.249.81.215 | Russian Federation | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 68.180.228.112 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 16 |
| 5.28.154.252 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 15 |
| 66.249.81.212 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 14 |
| 62.128.48.130 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 13 |
| 100.100.29.217 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 12 |
| 100.100.112.163 | | 147.237.72.156 | aman.idf.il | drop | First packet isn't SYN | drop | 12 |
| 5.22.134.154 | Israel | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 100.100.127.127 | | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 12 |
| 37.26.149.213 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 66.249.65.103 | United States | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 46.19.85.63 | Israel | 147.237.76.200 | eitan.aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 12 |
| 100.100.124.9 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 12 |
| 85.64.21.229 | Israel | 147.237.76.42 | refuah.idf.il | drop | First packet isn't SYN | drop | 11 |
| 54.244.22.103 | United States | 147.237.77.233 | atal.idf.il | drop | First packet isn't SYN | drop | 11 |
| 176.13.11.58 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 11 |
| 80.178.11.190 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 10 |
| 46.19.85.132 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 9 |
| 207.46.137.200 | United States | 147.237.77.178 | e.matpash.idf.il | Geo-location enforcement | Geo-location inbound enforcement | drop | 9 |
| 195.34.150.18 | Austria | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 208.115.111.73 | United States | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 108.49.74.166 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 96.81.67.33 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 9 |
| 188.209.52.109 | Romania | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 9 |
| 207.46.13.17 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 8 |
| 79.177.190.162 | Israel | 147.237.77.233 | atal.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 8 |
| 46.19.86.103 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 7 |
| 100.100.117.189 | | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 7 |
| 2.52.177.76 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 37.26.146.161 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.13.15.206 | Israel | 147.237.77.234 | halag.idf.il | Bad TCP sequence | SYN retransmit with different window scale | monitor | 6 |
| 212.117.140.158 | Israel | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 6 |
| 46.60.42.195 | Palestinian Territory Occupied | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 176.106.226.153 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | reject | 6 |
| 66.249.64.243 | United States | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |
| 79.176.124.217 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 6 |

11-24-2015-22:04:05 to 11-24-2015-23:04:05

| Attacker Address | Attacker Country | Target Address | Site | **Signature** | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 213.57.128.207 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |
| 46.19.86.103 | Israel | 147.237.77.226 | www.chamatz.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 6 |

11-24-2015-22:04:05 to 11-24-2015-23:04:05

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.67.214.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 86 |
| 2.54.140.214 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 77 |
| 109.67.214.24 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Too Many of the Same Response Code (404) | Block | 67 |
| 46.19.86.34 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 25 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 46.60.42.195 | Block | 17 |
| 84.108.194.134 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 13 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx | Block | 6 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx | Block | 6 |
| 2.54.26.143 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 85.250.123.44 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 46.19.85.221 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 79.179.123.63 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 2.54.186.174 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 3 |
| 77.127.169.22 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 85.64.202.120 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Distributed Illegal Parameter Encoding | None | 2 |
| 2.54.28.113 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 54.244.22.103 | United States | 147.237.76.147 | chinuch.aka.idf.il | Distributed Suspicious Response Code_Custom_Temporary | Block | 2 |
| 85.250.138.148 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 109.66.193.112 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api | Block | 2 |
| 5.22.134.154 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 79.183.218.83 | Israel | 147.237.0.19 | madim.atal.idf.il | Distributed Suspicious Response Code | Block | 2 |
| 66.249.78.52 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm | Block | 2 |
| 46.118.155.216 | Ukraine | 147.237.77.176 | matpash.idf.il | Multiple Unauthorized URL Access from 46.118.155.216 | Block | 2 |
| 80.178.139.2 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 212.179.152.234 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 46.166.190.168 | Netherlands | 147.237.77.216 | dover.idf.il | Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx. | Block | 1 |
| 109.64.131.189 | Israel | 147.237.76.42 | refuah.idf.il | Multiple Unauthorized URL Access from 109.64.131.189 | Block | 1 |
| 46.116.182.148 | Israel | 147.237.72.166 | aka.idf.il | Distributed PHP Attempt | Block | 1 |
| 95.211.196.17 | Netherlands | 147.237.0.15 | kosher-kravi.idf.il | URL is Above Root Directory kosher-kravi.idf.il/../shared/usercontrols/headerupper/ | Block | 1 |
| 46.19.85.253 | Israel | 147.237.77.216 | dover.idf.il | Illegal HTTP Version __atuvs=5654c3ebcec6c8e5000 | Block | 1 |
| 79.177.190.162 | Israel | 147.237.77.233 | atal.idf.il | Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx | Block | 1 |
| 176.106.227.81 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1381-he/dover.aspx | Block | 1 |
| 87.68.251.94 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 37.26.149.188 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 66.249.78.59 | Israel | 147.237.76.147 | chinuch.aka.idf.il | Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm | Block | 1 |
| 157.55.39.67 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp | Block | 1 |
| 2.54.187.17 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Unknown SSL Session | None | 1 |
| 66.220.158.111 | United States | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: sigalgs DoS Attack | None | 1 |
| 46.60.42.195 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.il | Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx | Block | 1 |
| 84.108.109.77 | Israel | 147.237.77.234 | halag.idf.il | Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif | Block | 1 |
| 221.231.6.246 | China | 147.237.77.74 | law.idf.il | Unauthorized HTTP Method | Block | 1 |
| 46.118.155.216 | Ukraine | 147.237.77.176 | matpash.idf.il | Unauthorized URL Access to www.cogat.idf.il/blog/ | Block | 1 |

11-24-2015-22:04:05 to 11-24-2015-23:04:05